IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2004 情財第 1094 号

広域インシデント情報共有および分析技術の開発

取扱説明書

2005 年 10 月

独立行政法人 **情報処理推進機構**

1. 広域インシデント分析・警戒システム 1

1.1. SIDA IODEF RECEIVER / ARCHIVER 1
1.2. SIDA IODEF GENERATOR 2
1.3. MANUAL AUTHORING 4
1.4. IODEF SENDER 4
1.5. IODEF RECEIVER / ARCHIVER 5
1.6. IODEF ANALYZER 9

2. 広域不正アクセス追跡システム 14

2.1. IODEF RIDSERVER 14
2.2. IODEF WIDE AREATRACKER 15

1. 広域インシデント分析・警戒システム

1.1. Sida IODEF Receiver / Archiver

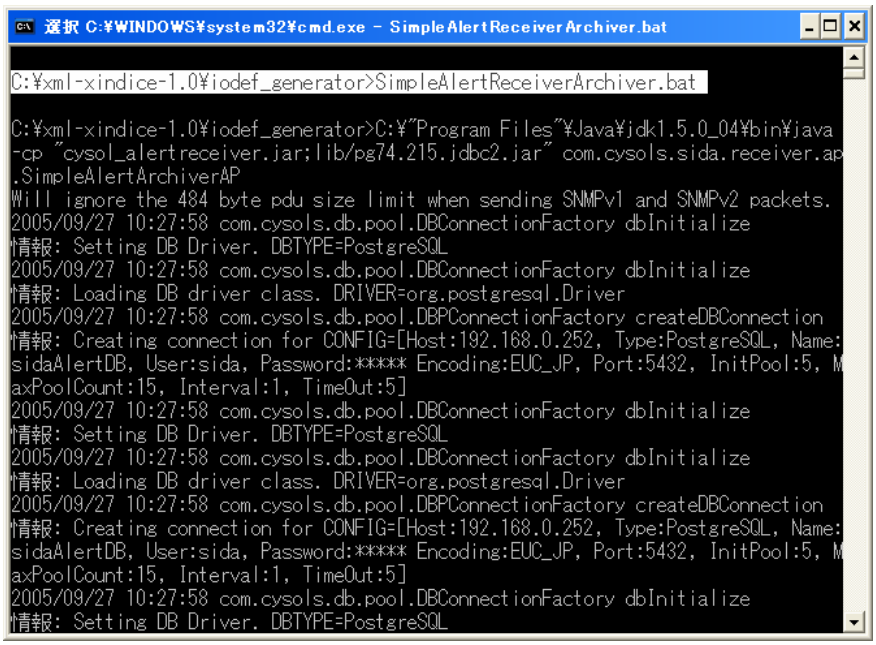
- サービス開始
  PostgreSQL Data Server 8.0 を実行します.

- config/AlertReceiver.conf の設定
  - ✧ SNMPPORT：162 - SNMP Trap/Notification のデフォルトポート，Snort アウトプットプラグインの設定に合わせて受信ポートを設定します.
  - ✧ DATA_DIR：data/を指定．DATABASE が無効の場合，このディレクトリに受信した Snort アラートの情報がログされます.
  - ✧ DATABASE：true を指定．これにより DB 保存が有効となります.

- config/db.properties の設定
  - ✧ HOSTIP：PostgreSQL のアドレスを指定します.
  - ✧ DBPORT：5432 を指定します（PostgreSQL のデフォルト）.
  - ✧ DATABASE：sidaAlertDB を指定します（作成した DB）.
  - ✧ USER：sida を指定します（作成した DB アカウント）.
  - ✧ PASSWORD：指定したパスワードを指定します.

- 実行
  SimpleAlertReceiverArchiver.bat を実行します.

Cyber Solutions Inc., All rights reserved


選択 C:¥WINDOWS¥system32¥cmd.exe - SimpleAlertReceiverArchiver.bat
C:¥xml-xindice-1.0¥iodef_generator>SimpleAlertReceiverArchiver.bat
C:¥xml-xindice-1.0¥iodef_generator>C:¥"Program Files"¥Java¥jdk1.5.0_04¥bin¥java
-cp "cysol_alertreceiver.jar;lib/pg74.215.jdbc2.jar" com.cysols.sida.receiver.ap
.SimpleAlertArchiverAP
Will ignore the 484 byte pdu size limit when sending SNMPv1 and SNMPv2 packets.
2005/09/27 10:27:58 com.cysols.db.pool.DBConnectionFactory dbInitialize
情報: Setting DB Driver. DBTYPE=PostgreSQL
2005/09/27 10:27:58 com.cysols.db.pool.DBConnectionFactory dbInitialize
情報: Loading DB driver class. DRIVER=org.postgresql.Driver
2005/09/27 10:27:58 com.cysols.db.pool.DBPConnectionFactory createDBConnection
情報: Creating connection for CONFIG=[Host:192.168.0.252, Type:PostgreSQL, Name:
sidaAlertDB, User:sida, Password:***** Encoding:EUC_JP, Port:5432, InitPool:5, M
axPoolCount:15, Interval:1, TimeOut:5]
2005/09/27 10:27:58 com.cysols.db.pool.DBConnectionFactory dbInitialize
情報: Setting DB Driver. DBTYPE=PostgreSQL
2005/09/27 10:27:58 com.cysols.db.pool.DBConnectionFactory dbInitialize
情報: Loading DB driver class. DRIVER=org.postgresql.Driver
2005/09/27 10:27:58 com.cysols.db.pool.DBPConnectionFactory createDBConnection
情報: Creating connection for CONFIG=[Host:192.168.0.252, Type:PostgreSQL, Name:
sidaAlertDB, User:sida, Password:***** Encoding:EUC_JP, Port:5432, InitPool:5, M
axPoolCount:15, Interval:1, TimeOut:5]
2005/09/27 10:27:58 com.cysols.db.pool.DBConnectionFactory dbInitialize
情報: Setting DB Driver. DBTYPE=PostgreSQL

1.2. Sida IODEF Generator

- daemon の実行

  ASPATHS の場所でコマンドプロンプトから実行します.

  ```
  perl ./as_paths_dNew.pl tmp/*
  ```

- config/db.properties の設定

  Sida Receiver/Archiver の設定と同一のものを共有します.

- config/sidaiodefgen.conf の設定

  - ✧ DOMAIN：IODEF 作成元（組織など）のドメイン名を指定します.
  - ✧ SOURCE_NAME：監視場所などを基に，ユニークなデータ元名称を指定します.
  - ✧ QUEUE_DIR：queue/（作成した IODEF XML ファイルの保存先ディレクトリを指定します）. 特に変更する必要はありません.
  - ✧ ERROR_DIR：invalid/（作成時に規約違反した IODEF XML ファイルの保存先ディレクトリを指定します）. 特に変更する必要はありません.
  - ✧ LIMIT：DB から 1 回で読み出す Snort アラートの上限数を指定します. こ

の指定が１つの IODEF XML ファイルに含まれるインシデント数にもなります.

- config/packetiodefaggr.conf の設定
  - ✧ DOMAIN：IODEF 作成元（組織など）のドメイン名を指定します.
  - ✧ SOURCE_NAME：監視場所などを基に, ユニークなデータ元名称を指定します.
  - ✧ QUEUE_DIR：queue/（作成した IODEF XML ファイルの保存先ディレクトリを指定します）. 特に変更する必要はありません.
  - ✧ ERROR_DIR：invalid/（作成時に規約違反した IODEF XML ファイルの保存先ディレクトリを指定します）. 特に変更する必要はありません.
  - ✧ DUMP_DATA_DIR：dumpdata/（作成時に使用するファイルの保存先ディレクトリを指定します）. 特に変更する必要はありません.
  - ✧ TIMEOUT：タイムアウト値を指定します.
  - ✧ SENSOR_ID：センサ ID を指定します.

- config/contact.xml の設定

<ContactList>タグの中に複数の<Contact>要素を指定可能です. 最低１つの<Contact>要素を指定してください. Contact の”contactrole”属性と”contacttype”属性は必須です. 以下に<Contact>の DTD を示します.

```
-----
=================================================================
==
    ===   Contact class                                       ===
    ===     - Name
    ===     - RegistryHandle
    ===     - PostalAddress
    ===     - Email
    ===     - Telephone
    ===     - Fax
    ===     - Timezone
    ===     - Contact (recursive)

=================================================================
==
    -->
```

<!ELEMENT Contact (Name?, Description*, RegistryHandle*, PostalAddress?, Email*, Telephone*, Fax?, Timezone, Contact*)>
<!ATTLIST Contact
contactrole (creator | admin | tech | irt | cc) #REQUIRED
contacttype (person | organization) #REQUIRED
restriction %attvals.restriction; #IMPLIED
>

- バッチ処理の設定
  SidaIODEFGenerator.bat
  PacketIODEFGenerator.bat

1.3. Manual authoring

- config/iodeftrans.conf の設定
  - ✧ SMTP_SERVER：メール送信に使用するメールサーバを指定します.
  - ✧ SENDER_ADDERSS：送信元 E メールアドレスを指定します.
  - ✧ RECIPIENT_ADDRESS：送信先 E メールアドレスを指定します（カンマ区切りで複数の送信先を指定可能です）.
  - ✧ COMPLETED_DIR：completed/（送信した IODEF XML ファイルを保存するディレクトリを指定します）. 特に変更する必要はありません.

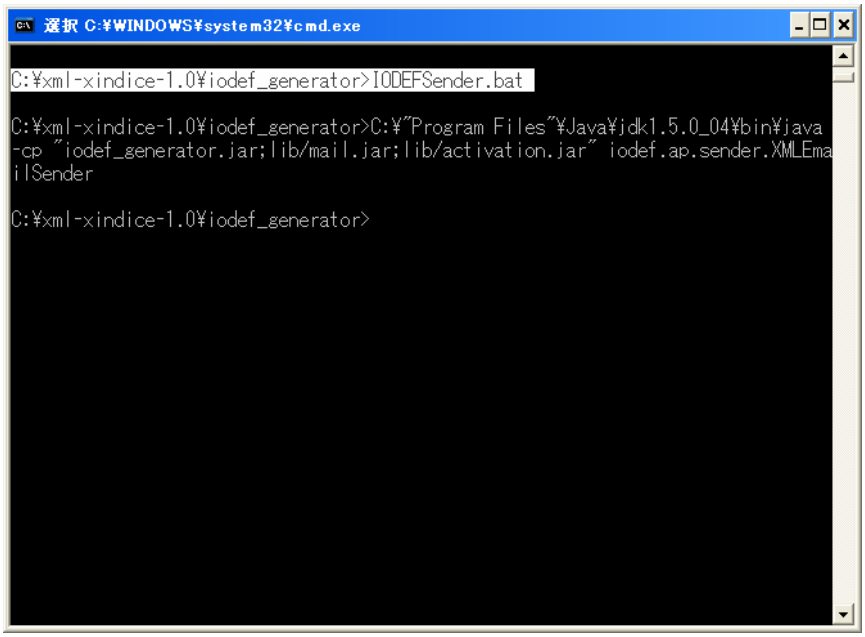
- バッチ処理の設定
  （次章 iodef_receiver の設定・起動後に実行する）
  ManualAuthoring.bat

1.4. IODEF Sender

- config/iodeftrans.conf の設定
  - ✧ SMTP_SERVER：メール送信に使用するメールサーバを指定します.
  - ✧ SENDER_ADDERSS：送信元 E メールアドレスを指定します.
  - ✧ RECIPIENT_ADDRESS：送信先 E メールアドレスを指定します（カンマ区切りで複数の送信先を指定可能です）.
  - ✧ COMPLETED_DIR：completed/（送信した IODEF XML ファイルを保存するディレクトリを指定します）. 特に変更する必要はありません.

Cyber Solutions Inc., All rights reserved

- バッチ処理の設定
  （次章 iodef_receiver の設定・起動後に実行する）
  IODEFSender.bat



1.5. IODEF Receiver / Archiver

- xindice の起動
  XINDICE_HOME/以下にある以下のコマンドより起動と終了が実行できます.

  起動

```
# XINDICE_HOME/startup
```

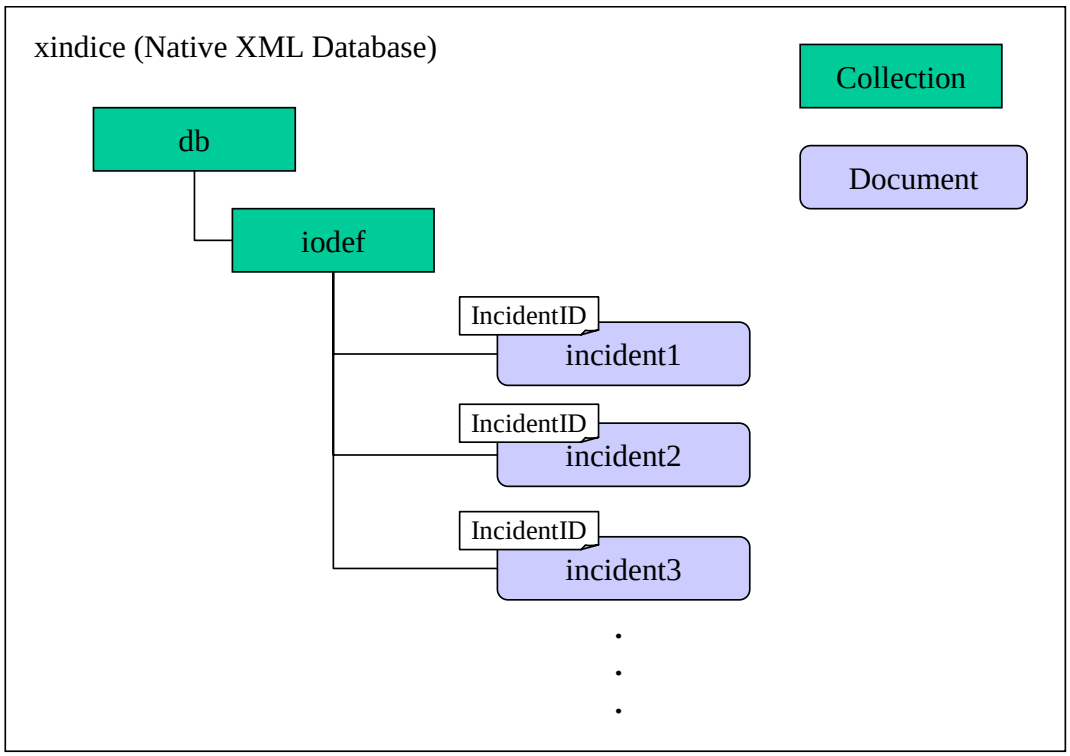
  終了

```
# XINDICE_HOME/bin/xindiceadmin shutdown -c /db
```

- xindice の設定
  xindice では XML 文書を“ Document ”といい Document はIDがつけられて Collection の下に格納されます. 本システムでは以下に示す iodef Collection に各インシデントを

Cyber Solutions Inc., All rights reserved

保存します.



db Collection は初期設定ですでに作成されているため，db 以下に/db/iodef Collection を以下のコマンドにより作成します.

```
# XINDICE_HOME/bin/xindiceadmin ac -c /db -n iodef
Created : /db/iodef
```

- 実行形式アーカイブ（config/db.properties）の設定
  IODEF Receiver/Archiver が使用する XML DB の設定をします．この設定を用いて Mailet から DB アクセスが行われます.
  - ✧ HOSTIP：xindice を実行しているマシンのアドレスを指定します.
  - ✧ DBPORT：4080（DB アクセスのポート番号を指定します）特に変更する必要はありません.
  - ✧ DATABASE：db（ルートの Collection を指定します）特に変更する必要はありません.
  - ✧ COLLECTION：iodef（IODEF 用の Collection を指定します）特に変更す

Cyber Solutions Inc., All rights reserved

る必要はありません.

- James (Java Apache Mail Enterprise Server)の設定
  IODEF 収集のためのセンター用実行形式アーカイブは James が含まれた状態で提供されます．すでに Mailet の設定もされているため，メールサーバとしての基本設定と IODEF XML ファイル受信用のアカウント設定を行います.

＜基本設定＞

James メールサーバ起動前に基本的な設定を行います．以下に基本的な設定箇所を示します．高度な設定は James のマニュアルを参照してください.

(1) apps/james/SAR-INF/config.xml の編集

<config>タグ内の以下のタグ要素を指定します.

- ✧ メールサーバ名：<James> ⇒ <servernames> ⇒ <servername>
- ✧ DNS サーバ：<dnsserver> ⇒ <servers> ⇒ <server>
  （ただし Windows XP の場合，dnsserver の audodiscovery は false にしなければなりません）
- ✧ リモートマネージャのアカウント：<remotemanager> ⇒ <handler> ⇒ <administrator_accounts> ⇒ <account>

(2) James の起動

以下のスタートスクリプトより James を起動します．/usr/local/iodef_center/ にパッケージを展開した例です．Windows の場合は”run.bat”を使用してください.
SMTP や POP のポートをオープンするために管理者権限が必要になります(Unix).

```
# /usr/local/iodef_center/bin/run.sh
Using PHOENIX_HOME:     /usr/local/iodef_center
Using PHOENIX_TMPDIR: /usr/local/iodef_center/temp
Using JAVA_HOME:          /usr/local/java
Running Phoenix:

Phoenix 4.0.1

James 2.2.0
```

Cyber Solutions Inc., All rights reserved

```
Remote Manager Service started plain:4555
POP3 Service started plain:110
SMTP Service started plain:25
NNTP Service Disabled
Fetch POP Disabled
FetchMail Disabled
```

(3) iodef アカウントの作成

リモートマネージャに接続してメールアカウントを作成します．リモートマネージャは 4555 ポート（デフォルト）に telnet 接続して利用します(起動時に Remote Manager Service としてポート番号が出力されます).

接続後にアカウントとパスワードを入力します．(1)で指定したものを入力してください（デフォルトでアカウント，パスワード共に root）.

```
# telnet <HOST ADDRESS> 4555
Trying 1<HOST ADDRESS>...
Connected to <HOST ADDRESS>.
Escape character is '^]'.
JAMES Remote Administration Tool 2.2.0
Please enter your login and password
Login id:
Password:

Welcome root. HELP for a list of commands
```

ログイン後に adduser コマンドにより iodef メールアカウントを作成します.
以下の例ではアカウント，パスワード共に iodef とします．作成後は listusers コマンドで確認できます.

```
adduser iodef iodef
User iodef added
```

Cyber Solutions Inc., All rights reserved

```
listusers
Existing accounts 1
user: iodef
```

＜実行＞

James の設定(2)によりメールサーバはすでに起動しています. 各観測点からの IODEF XML ファイル送信の設定を James の iodef アカウント宛に設定することで送信されたメールを受信し，添付の XML ファイルからインシデントを抽出して XML DB に格納します.

停止はリモートマネージャに接続して shutdown コマンドを実行することで可能です.

1.6. IODEF Analyzer

- Analyzer（config/db.properties）の設定

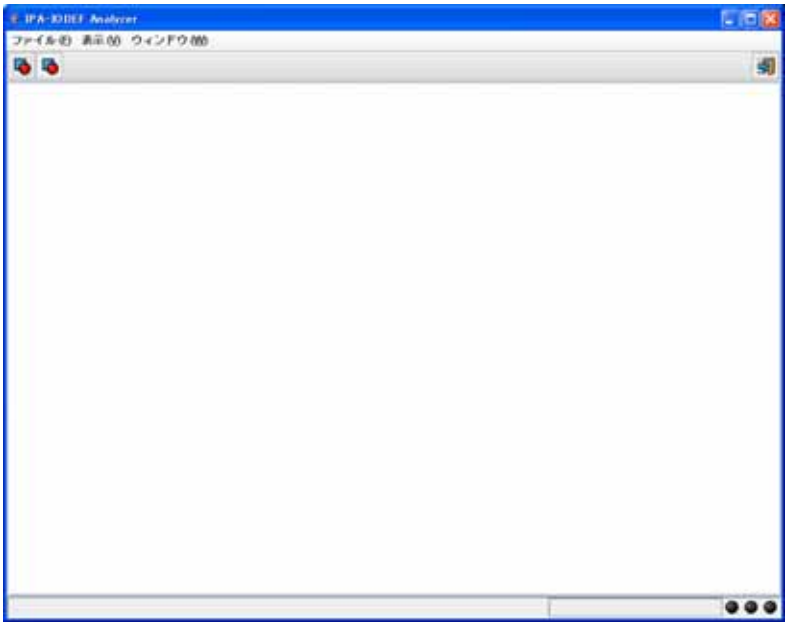
IODEF Analyzer が使用する XML DB の設定をします．この設定を用いて DB アクセスが行われます.

- ✧ HOSTIP：xindice を実行しているマシンのアドレスを指定します.
- ✧ DBPORT：4080（DB アクセスのポート番号を指定します）特に変更する必要はありません.
- ✧ DATABASE：db（ルートの Collection を指定します）特に変更する必要はありません.
- ✧ COLLECTION：iodef（IODEF 用の Collection を指定します）特に変更する必要はありません.

- 実行

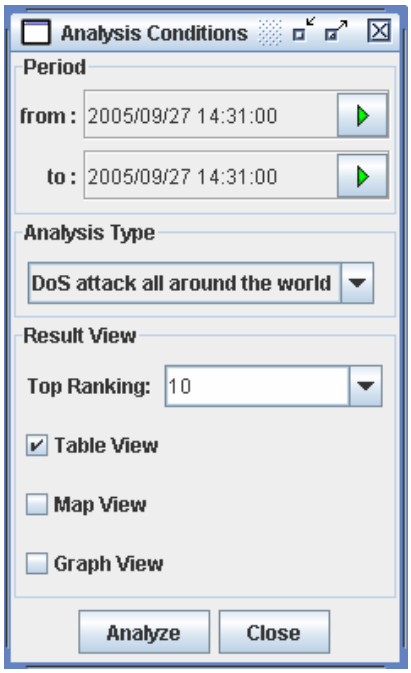
Analyzer.bat を実行します.

Cyber Solutions Inc., All rights reserved



1.6.1. Analysis Conditions

メニューバーの「ファイル」－「Incident Analysis」をクリックすると、「Analysis Conditions」が起動します。



アナライズの条件を指定できます。

- Period

▶ボタンをクリックすると、「日付 選択」が表示されます。年・月・日・時・分・秒を指定します。

・ Analysis Type

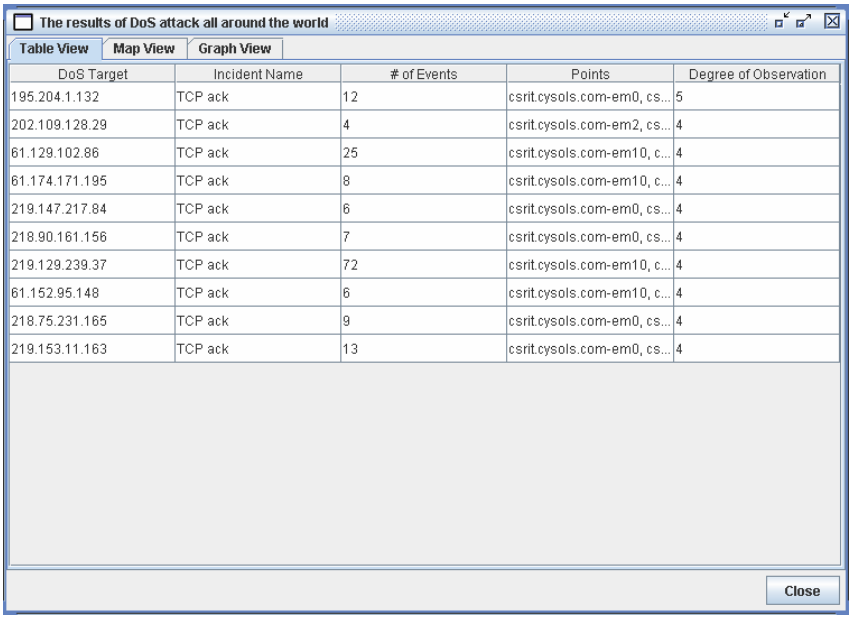
Analysis タイプ（Dos attack all around the world・Widely operated attacks）を選択します。

・ Result View

トップランク（Degree of Observation のトップランク）とビュー（Table View・Map View・Graph View※複数選択可）を選択します。

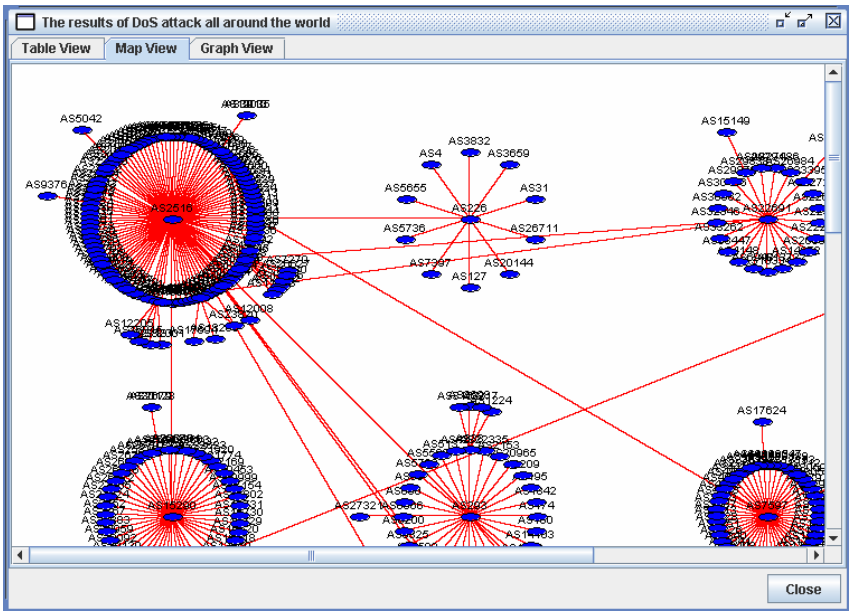
「Analyze」をクリックすると、指定した結果を表示します。

・ ビューで Table View を指定した結果

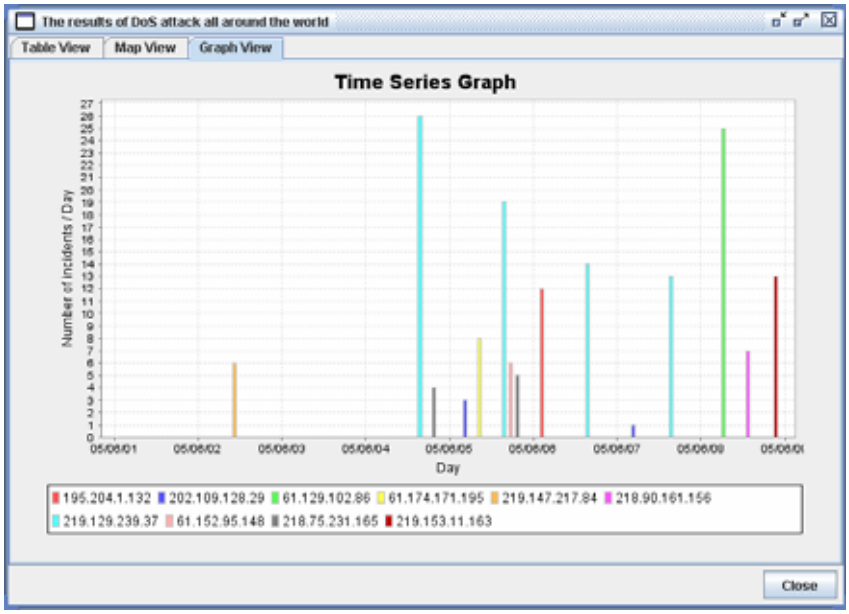

The results of DoS attack all around the world
Table View
Map View
Graph View
DoS Target | Incident Name | # of Events | Points | Degree of Observation
195.204.1.132 | TCP ack | 12 | csrit.cysols.com-em0, cs... | 5
202.109.128.29 | TCP ack | 4 | csrit.cysols.com-em2, cs... | 4
61.129.102.86 | TCP ack | 25 | csrit.cysols.com-em10, c... | 4
61.174.171.195 | TCP ack | 8 | csrit.cysols.com-em10, c... | 4
219.147.217.84 | TCP ack | 6 | csrit.cysols.com-em0, cs... | 4
218.90.161.156 | TCP ack | 7 | csrit.cysols.com-em0, cs... | 4
219.129.239.37 | TCP ack | 72 | csrit.cysols.com-em10, c... | 4
61.152.95.148 | TCP ack | 6 | csrit.cysols.com-em10, c... | 4
218.75.231.165 | TCP ack | 9 | csrit.cysols.com-em0, cs... | 4
219.153.11.163 | TCP ack | 13 | csrit.cysols.com-em0, cs... | 4
Close

Cyber Solutions Inc., All rights reserved

・ ビューで Map View を指定した結果



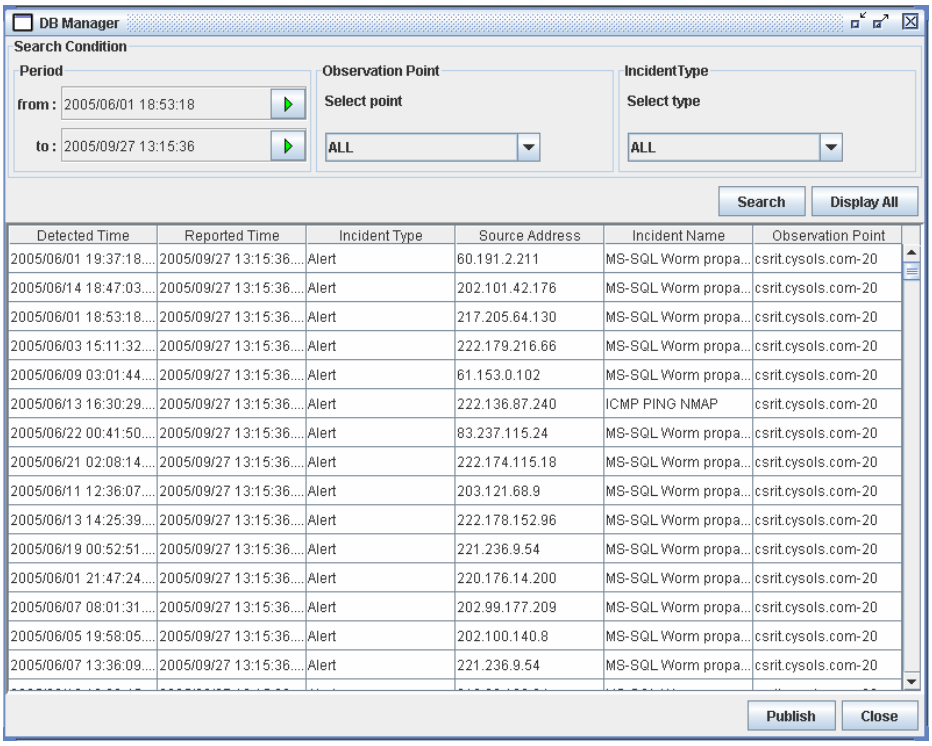
・ ビューで Graph View を指定した結果



1.6.2. DB Manager

メニューバーの「ファイル」－「DB Management」をクリックすると、「DB Manager」が起動します。

Cyber Solutions Inc., All rights reserved


DB Manager
Search Condition
Period
from : 2005/06/01 18:53:18
to : 2005/09/27 13:15:36
Observation Point
Select point
ALL
IncidentType
Select type
ALL
Search
Display All
Detected Time | Reported Time | Incident Type | Source Address | Incident Name | Observation Point
2005/06/01 19:37:18 | 2005/09/27 13:15:36 | Alert | 60.191.2.211 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/14 18:47:03 | 2005/09/27 13:15:36 | Alert | 202.101.42.176 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/01 18:53:18 | 2005/09/27 13:15:36 | Alert | 217.205.64.130 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/03 15:11:32 | 2005/09/27 13:15:36 | Alert | 222.179.216.66 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/09 03:01:44 | 2005/09/27 13:15:36 | Alert | 61.153.0.102 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/13 16:30:29 | 2005/09/27 13:15:36 | Alert | 222.136.87.240 | ICMP PING NMAP | csrit.cysols.com-20
2005/06/22 00:41:50 | 2005/09/27 13:15:36 | Alert | 83.237.115.24 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/21 02:08:14 | 2005/09/27 13:15:36 | Alert | 222.174.115.18 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/11 12:36:07 | 2005/09/27 13:15:36 | Alert | 203.121.68.9 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/13 14:25:39 | 2005/09/27 13:15:36 | Alert | 222.178.152.96 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/19 00:52:51 | 2005/09/27 13:15:36 | Alert | 221.236.9.54 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/01 21:47:24 | 2005/09/27 13:15:36 | Alert | 220.176.14.200 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/07 08:01:31 | 2005/09/27 13:15:36 | Alert | 202.99.177.209 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/05 19:58:05 | 2005/09/27 13:15:36 | Alert | 202.100.140.8 | MS-SQL Worm propa... | csrit.cysols.com-20
2005/06/07 13:36:09 | 2005/09/27 13:15:36 | Alert | 221.236.9.54 | MS-SQL Worm propa... | csrit.cysols.com-20
Publish
Close

検索条件を指定できます。

・ Period

▶ボタンをクリックすると、「日付 選択」が表示されます。年・月・日・時・分・秒を指定します。

・ Observation Point

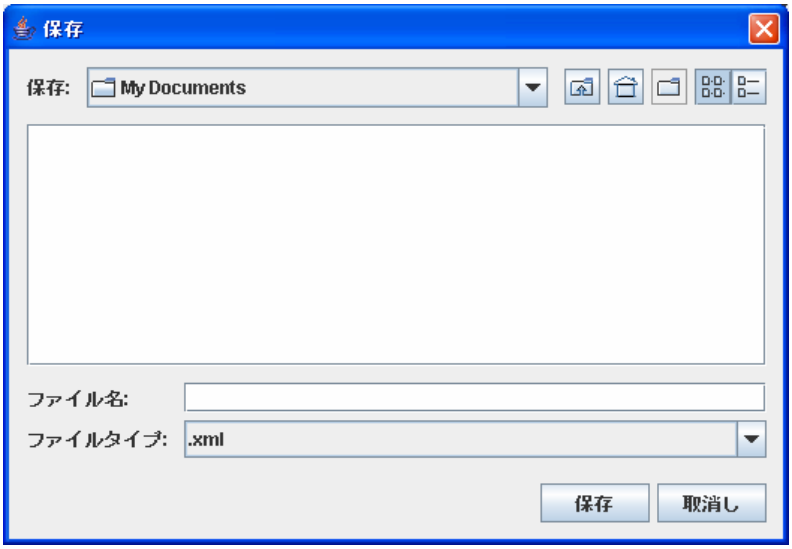
Observation Point を選択します。

・ Incident Type

Incident Type（ALL・Alert・Packet・Report）を選択します。

「Analyze」をクリックすると、指定した結果を表示します。「Display All」をクリックすると、DB のインシデントをすべて表示します。

選択した
「Publish」をクリックすると、「保存」が表示されます。選択したインシデントを指定した場所に保存できます。



2. 広域不正アクセス追跡システム

2.1. IODEF RidServer

- 実行
  $ bin¥catalina.bat start を実行，Tomcat(HTTP サーバ込み)を起動

  注意)カレントディレクトリは iodef_ridserver
  ※ 停止 $ bin¥catalina.bat stop

Cyber Solutions Inc., All rights reserved

2.2. IODEF Wide AreaTracker

- config/ridgen.conf の編集

  - ✧ DOMAIN：IODEF 作成元（組織など）のドメイン名を指定します.
  - ✧ SOURCE_NAME：監視場所などを基に，ユニークなデータ元名称を指定します.
  - ✧ NAME：送信元の組織名を指定します.
  - ✧ SRC_ADDRESS： 送信元の IP アドレスを指定します.
  - ✧ EMAIL：送信元のメールアドレスを指定します.
  - ✧ RID_QUERY_URL:/iodef_ridserver/services/RIDQuery(RID サーバの URL を指定します)．特に変更する必要はありません.
  - ✧ MAP_FILE：config/map/map.disp（map ファイルの読み取り元を指定します)．特に変更する必要はありません.
  - ✧ DST_ADDRESS-0:RID サーバを起動したホストとポート番号を指定します.

- config/AlertRecever.conf の編集
  - ✧ SNMPPORT：162 - SNMP Trap/Notification のデフォルトポート，Snort アウトプットプラグインの設定に合わせて受信ポートを設定します.
  - ✧ DATA_DIR：data/を指定．DATABASE が無効の場合，このディレクトリに受信した Snort アラートの情報がログされます.

- daemon の実行

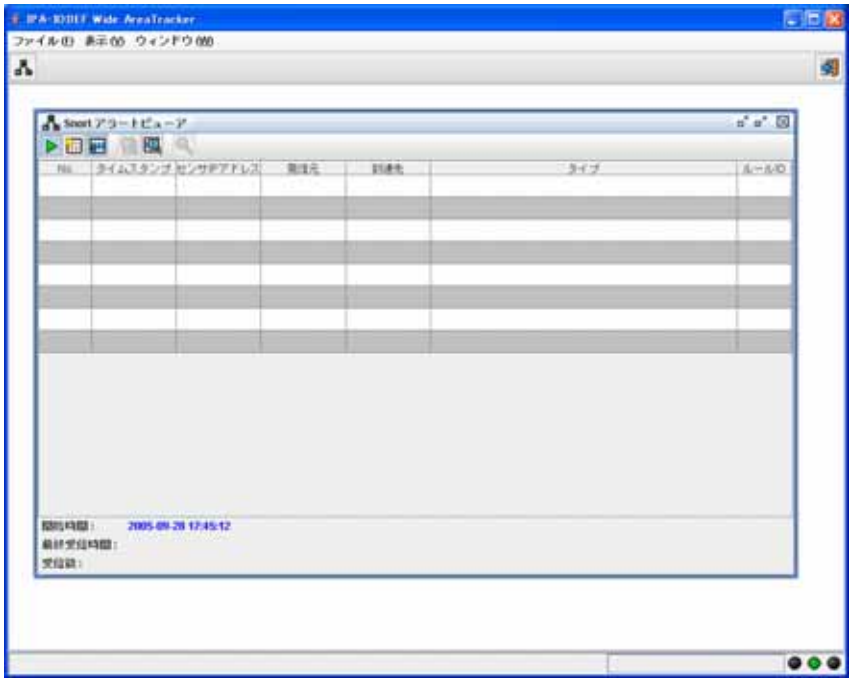
  ASPATHS の場所でコマンドプロンプトから実行します.

```
perl ./as_paths_dNew.pl tmp/*
```

- 実行

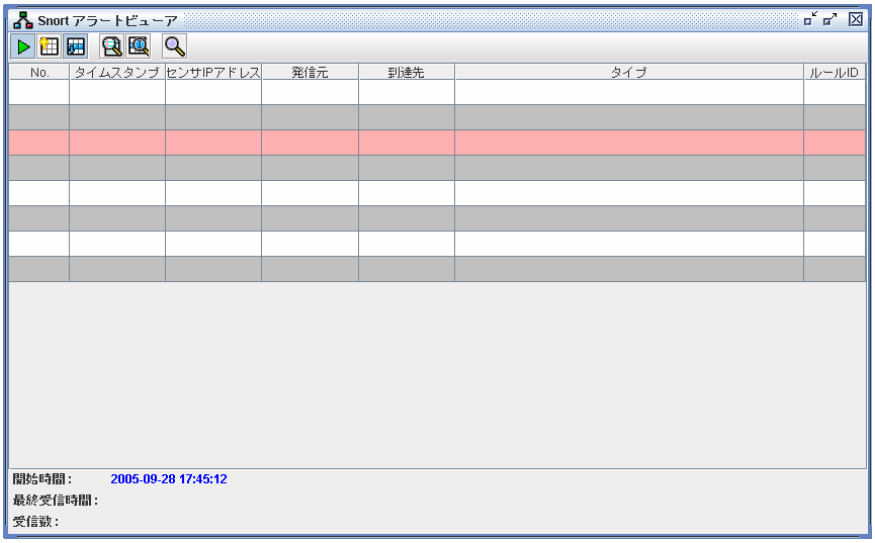
  WideAreaTracker..bat を実行します.

Cyber Solutions Inc., All rights reserved



2.2.1. Snort アラートビューア

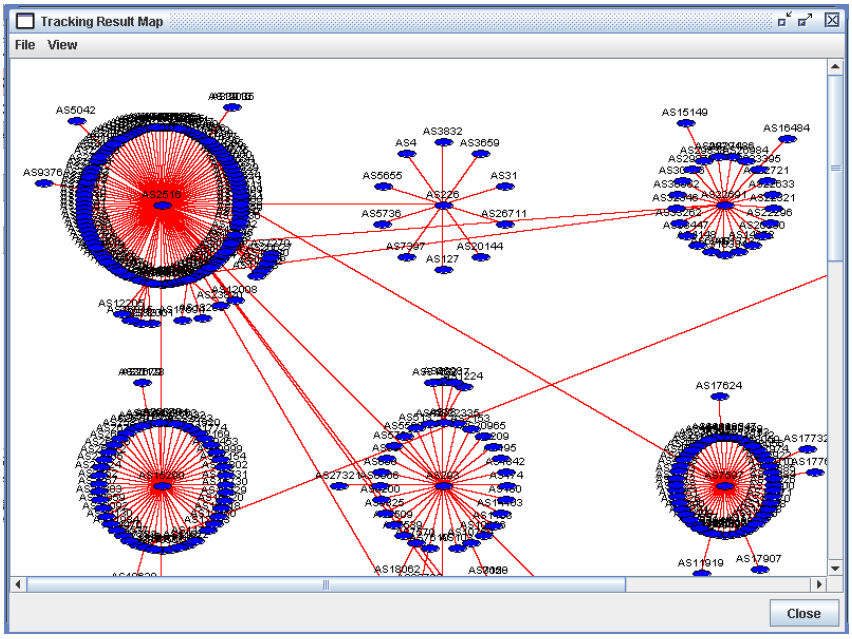
メニューバーの「ファイル」－「Snort アラートビューア」をクリックすると、「Snort アラートビューア」が起動します。



	アラート表示中に表示されます 選択することでアラート表示を停止します
	アラート表示停止中に表示されます 選択することでアラート表示を開始します
	アラートテーブルの内容をクリアします
	アラートテーブルの自動スクロールが無効の際に表示されます 選択することで自動スクロールを有効にします
	アラートテーブルの自動スクロールが有効の際に表示されます 選択することで自動スクロールを無効にします
	アラートテーブル上の選択されたアラートの詳細を表示します
	表示するデータを選択します
	RID Query が RidServer に送られます

sidaMIB alert を受信します。一覧表示されたものを選択して、 ボタンをクリックすると RID Query が RidServer に送られます。「Tracking Result Map」を表示します。

Cyber Solutions Inc., All rights reserved



Cyber Solutions Inc., All rights reserved